PCT

WORLD INTELLECTUAL PROPERTY ORGANIZATION
International Bureau

INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(51) International Patent Classification 6 : H04K 1/00	A1	(11) International Publication Number: WO 95/23465 (43) International Publication Date: 31 August 1995 (31.08.95)

(21) International Application Number: PCT/US95/02007

(22) International Filing Date: 17 February 1995 (17.02.95)

(30) Priority Data:

08/201,106	23 February 1994 (23.02.94)	US
08/303,048	8 September 1994 (08.09.94)	US

(71) Applicant: BELL COMMUNICATIONS RESEARCH, INC. [US/US]; 290 West Mount Pleasant Avenue, Livingston, NJ 07039-2729 (US).

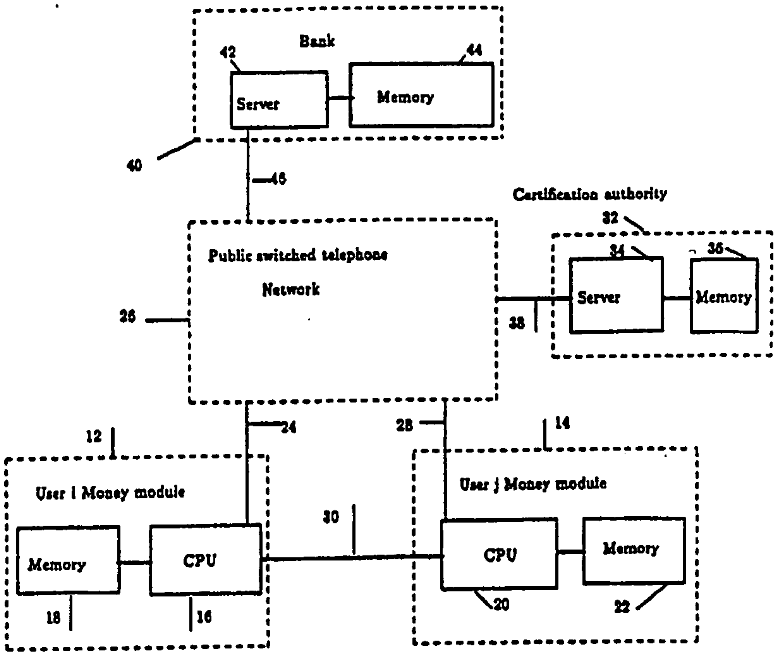
(72) Inventor: YACOBI, Yacov; 23 Lenape Lane, Berkeley Heights, NJ 07922 (US).

(74) Agents: YEADON, Loria, B. et al.; International Coordinator, Room 2D-312, 290 West Mount Pleasant Avenue, Livingston, NJ 07039-2729 (US).

(81) Designated States: CA, JP, European patent (AT, BE, CH, DE, DK, ES, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE).

Published
With international search report.

(54) Title: EFFICIENT ELECTRONIC MONEY



(57) Abstract

A unique electronic cash (14) system protects the privacy of users (12) in legitimate transactions while at the same time enabling the detection (32) of a double spender of the same electronic coin (14). The electronic cash system takes advantage of a unique property of El Gamal signatures to achieve these results.

FOR THE PURPOSES OF INFORMATION ONLY

Codes used to identify States party to the PCT on the front pages of pamphlets publishing international applications under the PCT.

AT	Austria
AU	Australia
BB	Barbados
BE	Belgium
BF	Burkina Faso
BG	Bulgaria
BJ	Benin
BR	Brazil
BY	Belarus
CA	Canada
CF	Central African Republic
CG	Congo
CH	Switzerland
CI	Côte d'Ivoire
CM	Cameroon
CN	China
CS	Czechoslovakia
CZ	Czech Republic
DE	Germany
DK	Denmark
ES	Spain
FI	Finland
FR	France
GA	Gabon
GB	United Kingdom
GE	Georgia
GN	Guinea
GR	Greece
HU	Hungary
IE	Ireland
IT	Italy
JP	Japan
KE	Kenya
KG	Kyrgystan
KP	Democratic People's Republic of Korea
KR	Republic of Korea
KZ	Kazakhstan
LI	Liechtenstein
LK	Sri Lanka
LU	Luxembourg
LV	Latvia
MC	Monaco
MD	Republic of Moldova
MG	Madagascar
ML	Mali
MN	Mongolia
MR	Mauritania
MW	Malawi
NE	Niger
NL	Netherlands
NO	Norway
NZ	New Zealand
PL	Poland
PT	Portugal
RO	Romania
RU	Russian Federation
SD	Sudan
SE	Sweden
SI	Slovenia
SK	Slovakia
SN	Senegal
TD	Chad
TG	Togo
TJ	Tajikistan
TT	Trinidad and Tobago
UA	Ukraine
US	United States of America
UZ	Uzbekistan
VN	Viet Nam

EFFICIENT ELECTRONIC MONEY

Related Application

This is a continuation-in-part of U.S. Patent Application Serial No. 08/201,106 filed on February 23, 1994 for Y. Yacobi and assigned to the assignee hereof.

Field of the Invention

The present invention relates to electronic money, specifically, to a form of electronic money which is the electronic equivalent of cash. The invention provides a form of electronic money which deters double spending of a specific electronic coin, while at the same time protecting the privacy of payers (spenders) and payees (recipients) in cash transactions.

Background of the Invention

Electronic money (e-money) comes in the same forms as ordinary money. For example, there are electronic equivalents of checks (e-checks) and electronic equivalents of cash (e-cash).

Electronic checks are easier to implement than electronic cash. In a paper check, the most important component is the user's signature. This signature is supposed to insure the correctness of an obligation to transfer a certain amount of money from the signer ("payer") to a specified payee. In addition, certain properties of the paper of which the check is made are designed so that changes to the content of the paper check will be noticeable. All of these properties are inherent to digital signatures (see e.g., W. Diffie, M. Hellman, "New Directions in Cryptography" IEEE Trans. IT. 1976 and R. Rivest, A. Shamir, and L. Adelman, "A Method for Obtaining Digital Signatures and Public Key Cryptosystems", CACM, vol. 21, 1978, pp. 120-126). Thus, it is straightforward to implement digital checks. Similarly, it is easy to implement digital credit cards.

A digital signature in this case indicates the authenticity of the user and the user's consent to a particular transaction.

It is harder to create the digital equivalent of cash. (For a discussion of e-cash, see e.g., D. Chaum, et al. "Untraceable Electronic Cash", Proc. Crypto 1988, D. Chaum "Achieving Electronic Privacy" Scientific American, August 1992, pp 96-101, S. Brand "Electronic Cash Systems Based on the Representation Problem in Groups of Prime Order" Proceedings of Crypto '93 Santa Barbara 1993 pp 26-26.15; S. Even et al. "Electronic Wallet" Proc. Crypto '83). The main problem is this. Suppose that a bunch of digital bits represents a coin. What can prevent the payer from double spending the digital coin?

Two approaches have been used in the prior art to resolve this problem. Prevention and after the fact detection. For example, to prevent double spending, tamper resistant devices may be used. Such devices, called electronic wallets (e-wallets) or money modules, store a user's balance in a manner so that even the owner of the device cannot illegally modify the balance. A balance on one of these money modules can change if two such devices "agree" to a specified transaction, whereby one money module (the payer) agrees to pay X dollars to another money module (the payee). In this case, the balance in each money module is changed so that the sum of the two balances remains unchanged. A transaction between a bank and a user is similar except that it involves additional steps such as moving money from the user's checking account into the user's money module where the money now becomes e-cash. The use of tamper-resistant devices, i.e. money modules, to prevent the double spending of e-cash is preferred by banks because banks want to prevent double spending, not detect double spending after such double spending occurs.

However, it is impossible to create a 100% tamper proof money module type device. It is only a question of resources devoted to reverse engineering and description, etc. If by unwrapping one money module one could forge ten million dollars, then it makes economic sense (but not moral sense) to invest one million dollars to penetrate the money module. There is a spectrum of tamper-resistant technologies that range in price and quality and some economic optimum must be reached.

This optimum is less expensive if a second line of defense can be added. Such a second line of defense might be the use of a process which provides for after the fact exposure of the double spender.

Another issue that arises in connection with the use of e-cash is privacy. For large transactions (e.g. buying a house), traceable forms of e-money such as e-checks can be used. Usually these kinds of transactions are not viewed as secret transactions and usually the parties want evidence as to these transactions. Electronic cash (e-cash) is generally used for smaller daily transactions (e.g. buying groceries and buying newspapers, etc.). A user would not want a government or large private agency (e.g. a bank) to be able to constantly know his/her whereabouts and the details of daily purchases based on the payment of e-cash to various payees. Thus, after ordinary legitimate uses, the identity of an e-cash spender should not be traceable. On the other hand, the e-cash system should enable detection of the identity of a double spender of the same e-coin.

It is an object of the present invention to provide e-cash or e-coins with certain highly desirable characteristics. The characteristics include the following:

1. Once a bank detects double spending (i.e. the same e-coin is deposited twice), the bank should have enough information to efficiently expose the identity of the double spender. However, one legitimate deposit of a particular e-coin should not provide the bank with enough information to compute the identity of the person who paid the particular e-coin to the depositor.
2. The e-cash should be useable in the following transactions; (a) payment from payer to payee without revealing identity of payer, (b) deposit of money into

the bank by the payee without revealing the identity of the payer, (c) an exchange transaction wherein a depositor gets a certain amount of fresh money from the bank in exchange for depositing the same amount of old money into the bank without revealing his/her identity, and (d) withdrawal from the bank.

3. The system should be efficient. Specifically, the system should require as few real time operations as possible during transactions, especially at the money modules used by individual users as the money modules have limited processing power. As many operations as possible should be done in advance of and apart from the transactions which take place in real time.

The present invention provides an e-cash system which has these advantages.

The e-cash system of the present invention relies on certain prior art techniques. These prior art techniques are described below:

A. Public Key Cryptography

In a typical public key cryptographic system, each party i has a public key P_i and a secret key S_i. The public key P_i is known to everyone, but the secret key S_i is known only to party i. A clear text message m to user i is encrypted to form the cipher text message c using a public operation P which makes use of the public key P_i known to everyone, i.e., $c=P(m,P_i)$. The cipher text message c is decrypted using a secret operation S which makes use of the secret key S_i, i.e., $m=S(c,S_i)$. Only the party i which has the secret key S_i can perform the secret operation to decrypt the encrypted message.

Public key cryptographic techniques may also be used for authentication. If it is true that $P(S(m,S_i),P_i) = m$, then the owner of the corresponding keys P_i, S_i could sign message m by producing $s=S(m,S_i)$, where s indicates the signature. The verifier, given m and s will verify $m=P(s,P_i)$. A signature system could be used for verification as follows: Challenge the party claiming to be i with message m and ask the party to sign the message m using his secret key S_i, then verify the signature using P_i.

An example of a public key cryptographic technique is the well known RSA technique. In accordance with this technique, a party i has a public key in the form of an exponent e and modulus N and a secret key in the form of an exponent d. Thus,a party with a message to send to party i encrypts the message m to form $c \equiv m^e$ mod N. The party i can then decrypt c to obtain m by performing the operation $m=c^d$ mod N.

Another public key crytographic technique is the Rabin modular square root. In this technique, the secret operation involves obtaining a modular square root and the public operation involves a modular squaring operation.

B. EL Gamal Signature Scheme

Let P_i and S_i be the public and secret keys of user i, where

$P_i = \alpha^{si}$ mod p, where p is a large prime or a product of large primes, and α is a generator in Z^*_p. An El-Gamal signature by user i, on message m is an ordered pair s=(u,v), for which

$$P_i^u \;.u^v \equiv \alpha^m \bmod p \tag{1}$$

Thus a recipient of a signature can easily verify it. To create a signature, user i chooses a random number r, and computes $u = \alpha^r$ mod p. From eq (1) it follows that:

$$S_i \;.\; u + r \;.\; v \equiv m \bmod p - 1 \tag{2}$$

Hence i, who is the only one who knows S_i, can compute v, provided gcd(r,p - 1) = 1. The El Gamal signature scheme is disclosed in T. El Gamal "A Public Key Cryptosystem and a Signature Scheme Based on Discrete Logarithms", IEEE Trans IT, Vol. IT-31, No. 4, July, 1985, pp. 469-472.

The El-Gamal signature system has the curious property that if the signer i tries to use the same r twice to sign two different messages, then these two signatures expose his secret key S_i. To see how double use of r exposes S_i, note that from eq (2) that

$$S_i \ . \ u+r \ . \ v_1 \equiv m_1 \bmod p-1; \ S_i \ . \ u+r.v_2 \equiv m_2 \bmod p-1 \qquad (3)$$

Hence,

$$r(v_1-v_2) \equiv (m_1- m_2) \bmod p-1 \qquad (4)$$

If gcd $(v_1 - v_2, p-1) = 1$, anybody knowing the messages m_1, m_2 and their signatures (u,v_1), (u,v_2) can find r, and if gcd(v,p-1) =1, then S_i can be computed. This unique property of the El Gamal signature scheme is used as the basis for an e-cash system according to the invention in which the identity of a double spender of a particular e-coin is exposed. Other signature schemes such as NIST, DSS and Schnorr also have the property that if two distinct messages are signed using the same random element (e.g. r), then the secret key of the signer can be computed by anyone having the message, the signature and public information such as the public key of the user. Signature schemes with this property belong to the El Gamal family of signature schemes.

C. Blind Signature

The idea of a blind signature is to mimic a situation in which a person signs a closed envelope. The envelope includes some document and a carbon paper, so that the signature appears (via the carbon paper) on the document, without the signer knowing the contents of the document. The recipient can later fetch the signed document from the envelope. This seemingly bizarre idea proves very helpful in establishing nontraceability. A blind signature may be implemented using RSA as follows. The signer is associated with N,e,d (public modulus, public exponent, and secret exponent, respectively). The secret message to be signed is m. The recipient picks a random $x \in Z^*_N$, and presents a "message-in-envelope" $c \equiv x^e. m \bmod N$ to the signer, who signs it, i.e. computes $c^d \equiv x. m^d \bmod N$, from which the recipient, and only the recipient (who knows x), can compute the signed message $m^d \equiv c^d x^{-1} \bmod N$.

The public key cryptography techniques described above are used to provide a unique e-cash system according to the invention.

SUMMARY OF THE INVENTION

In accordance with an illustrative embodiment of the present invention, an e-cash system has four players. These are a certification authority, a bank, a payer also known as user i, and a payee also known as user j. There are six basic operations which may be carried out in the e-money system. These are: Initial Certificate, Receipt Certificate, Withdrawal, Payment, Deposit and Exchange. The elements of the e-money system of the present invention and the operations are discussed below.

Public Key and Secret Key

A user i has a public key, where for example, $P_i = \alpha^{si} \bmod p$, where α and p are universally known. S_i is a secret key of the user i. The secret key S_i includes the identity I_i of the user i. Illustratively, S_i is a concatenation of the user's name I_i and a string of random bits R_i known only to the user i, i.e., $S_i = (I_i, R_i)$. Alternatively, the secret exponent key S_i may include multiple copies of I_i. It should be noted that P_i and S_i are El Gamal public and secret keys respectively. As is shown below, this feature is important for detecting the identity of a double spender of a particular e-coin.

Alternatively, P_i and S_i are El Gamal public and secret keys and may be keys from a different signature scheme in the El Gamal family of signature schemes. However, it is desirable for S_i to contain the user's identity I_i.

Certification of the Public Key

The user may also have a certificate of the public key P_i. A certificate of a public key is a linkage between a user's identity I_i and the user's claimed public key P_i. In the present invention, this certificate is a proof that the public key P_i is legitimate and that the user's identity is embedded in the exponent or otherwise embedded in the public key. The certificate is, for example, a signature (e.g. an RSA signature) of a trusted authority on $f(P_i, 0^\gamma)$, where 0^γ denotes a run of γ zeros. The certificate of P_i is illustratively computed off-off line. The use of the function f is entirely optional. Thus, in some embodiments of the invention $f(P_i, 0^\gamma) = (P_i, 0^\gamma)$. In other embodiments of the invention, f is a publicly known collision free has function. Specifically, let $l(p) = \log_{<}(p)\gamma$. Let $\Sigma = \{0,1\}^{l(p)}$ and $f: \Sigma \rightarrow \Sigma$ be a publicly known collision free one way has function. (Sometimes f is used for $\Sigma = \{0,1\}^{l(p2)}$ and this is clear from the context.

As used herein the term "off-off line" designates operations which are performed rarely. Specifically, the term "off-off line" designates operations which may be performed once and whose results are used in many real time operations. The "off-off line" operations are to be contrasted with "off-line" operations which are used in on/off line digital signature schemes. In an on/off line digital signature scheme, for each real time digital signature to be performed, as much of the computation as possible is performed ahead of time to reduce real time computation. The computations performed ahead of time for each real time digital signature are referred to as "off-line" computations. There is a one-to-one correspondence between a set of "off-line" computations and a real time digital signature. In contrast, there is no one-to-one correspondence between "off-off" line computations and a real time operation. Rather, the results of an "off-off line" computation can be used in many subsequent real time operations. The use of "off-off line" operations is a unique feature of the present invention. It is a significant advantage of the invention, that the secret key P_i and its certificate can be computed "off-off line".

The certificate is obtained as follows. A candidate certificate $f(P_i, 0^\gamma)$ is blinded by computing $Z \equiv x^{ec} f(P_i, 0^\gamma) \bmod N_c$, where x is a random number, e_c is the public RSA exponent key of a trusted certificate authority, and N_c is a public modulus of the certificate authority. The quantity Z is then transmitted from the user i to the certificate authority.

The user i then proves to the certificate authority that P_i has been properly formatted, i.e., that the secret key S_i in the exponent of P_i includes the user identity I_i. This proof is can be accomplished without revealing P_i to the certificate authority so that the certificate authority cannot correlate I_i and P_i for the user i. If the certificate authority is able to correlate I_i and P_i, then the certificate authority will be able to gain knowledge of all the transactions performed by user i using e-cash. In the present invention, the identity of the user is exposed only when a coin is double spent. To prevent such a correlation, the candidate certificate is blinded before it is sent to the certificate authority. One technique which can be used to perform the proof is known as a zero-knowledge proof (see Goldreich, Micali, and Wigderson, Proofs that yield nothing, but their validity, or All languages in NP have zero-knowledge proof systems. J. of the ACM, 38: 691-729, 1991 and Goldwasser, Micali, and Rackoff, The knowledge complexity of Interactive proof systems, SIAM J. on Computing, 181, 1989, pp. 186-208, the contents of which are incorporated herein by reference). A zero knowledge proof can be used here because all of the predicates used in the proof are NP (Non-deterministic polynomial time). Another proof technique is to a "cut-and-choose" technique. The latter technique is discussed in detail below.

Assuming the proof is acceptable to the certificate authority, the certificate authority computes Z^{dc}, where d_c is the secret RSA exponent key of the certificate authority. Z^{dc} is then transmitted from the certificate authority to the user i, who then computes the certificate cert(i) = $Z^{dc}/x \equiv f(P_i, 0^{\gamma})^{dc}$ mod N_c. In short, the user i gets a certificate from the certificate authority that establishes a linkage between I_i and P_i. However, in contrast to ordinary certificates, this linkage is hidden. The user identity I_i is embedded in the discrete log of the public key P_i and is only exposed when there is double spending of a coin. Note that the certificate cert(i) may be periodically refreshed using off-off line computations.

Format of e-coin

In general, a coin includes a certified linkage between a public of a user and a random element. In accordance with an illustrative embodiment of the present invention, a coin of user i is represented by (Pi, u C) where the certified linkage C $\equiv f(P_i, u, 0^{\gamma})^{d\$}$ mod $N_\$$, where u $\equiv \alpha^{r}$ mod p, where r is a random element and is chosen by i and known only to i, $30 < \gamma < 50$, $d_\$$ is a bank's RSA secret exponent for coins of a particular denomination, and $N_\$$ is the RSA modulus of the bank. The key P_i, the value u, the modulus $N_\$$, and the public RSA exponent $e_\$$ (corresponding to the secret RSA exponent $d_\$$) are known publicly. Each coin of user i has a different value of the random element r, but the same P_i is used in many coins.

The following on-line (i.e. real time transactions) can be performed using the e-cash of the present invention.

1. Payment

The payer i transmits a coin (P_i,u,C), where the certified linkage C $\equiv f(P_i, u, 0^{\gamma})^{d\$}$ mod $N_\$$ to the payee j. The payee j verifies the bank's signature by verifying $C^{e\$} \equiv (P_i$ u, $0^{\gamma})$ mod $N_\$$. If the banks' signature is correct, the payee j challenges the payer i to sign a random message m using (P_i, u) embedded in the coin using an El Gamal signature or some other signature from the El Gamal Family. The payer i computes the El Gamal signature s=(u,v) and transmits the signature to the payee

j. The payee j then verifies the El Gamal signature. The payee j now stores the coin.

In short, in the payment operation the payer sends a coin (certified linkage between a public key and a random element) to a payee. The payee verifies the certificate which illustratively is a banks signature. The payee then challenges the payer to sign a message m using a signature scheme for the El Gamal family, using the public key and random element embedded in the coin. The payee then verifies the signature.

2. Deposit

Suppose the payee j wants to deposit the coin C (P_i,u,C) in the bank. The payee j transmits the coin (P_i,u,C) and the El Gamal signature (u,v) of the payer i to the bank. The message m that was signed by payer i is also transmitted to the bank. The bank verifies the coin by verifying that $C^{e\$} \equiv f(P_i, u, 0^{\gamma}) \bmod N_{\$}$.

The bank maintains a list of deposited coins (P^i, u, C^{γ}) and corresponding El Gamal signatures (u,v) and messages m.

The bank then compares the coin currently being deposited with the coins in the list. If there is a duplicate,using equations (2) and (3) above, r and S_i can be determined. From S_i, the identity I_i of the double spender is exposed. If there is no duplicate, the coin is added to the list and the balance of the payee j is updated. The list of coins will not grow endlessly if an expiration date is embedded in the coins.

In short, in the deposit operation, the payee transmits the received coin and the payer's El Gamal family signature to the bank. The bank verifies the coin and then compares the coin to a list of previously deposited coins to see if the coin was deposited in the past. If the coin was deposited in the past, the bank is able to determine the identity of the double spender. Specifically, the bank would have received two El Gamal family signatures on two different messages but using the same random element.

Exchange of Old Money for New

Instead of the payee j simply depositing the coin received form the payer i, the payee j can deposit the coin C at the bank and ask for new coins of the same total value in return. The deposit routine as described above is performed and a check is made for double spending but no change is made to j's balance. The payee j transmits to the bank a non-blinded certificate $(P_j, 0^{\gamma})^{dc}$ mod N_c which then verifies P_j. For each requested coin, the payee also sends to the bank $u = \alpha^{r'}$ mod p of his choice. The user j gets back from the bank $C' \equiv f(P_j,\ u,\ 0^{\gamma})^{d\$}$ mod $N_{\$}$. The exchange transaction is a feature of the present invention which is not found in prior out e-money systems.

In short, in the exchange operation, a payee deposits old coins in the bank and gets fresh coins in the same total value from the bank. The payee does reveal his/her identity to the bank and the linkage (user, coin) is not known to the bank.

Withdrawal

Another operation which can be performed is a withdrawal operation. According to this operation, the user i establishes communication with the bank and authenticates himself/herself with the bank. The user i presents a candidate blinded coin $w \equiv x^{e\$}\ f(P_i,\ u,\ 0^{\gamma})$mod $N_{\$}$ on which it is desired to obtain the banks RSA signature. The user also proves to the bank (using a zero knowledge proof, or cut-and-choose proof, for example) that P_i is properly structured without revealing the key P_i to the bank so that the bank cannot correlate the user i with P_i. The bank deducts the value of the coin from the user's balance. The bank then returns $w^{d\$}$ mod $N_{\$}$, from which the user can compute a coin (P_i, u, C), where the certified linkage $C = f(P_i,\ u,\ 0^{\gamma})^{d\$}$ mod $N_{\$}$. It is expected that the exchange operation will be used more frequently than the more complex withdrawal operation.

In short, in the withdrawal operation a blinded linkage between a public key (e.g. P_i) and a random element (e.g. u) is transmitted to the bank. Blinding is used because the user's ID (e.g. I_i) is exposed to the bank. The bank verifies that P_i is properly structured (i.e. the user's identity I_i (reembedded therein). The bank then signs the blinded linkage and returns the signed blinded linkage to the user who then computes a coin.

The inventive e-cash system disclosed above has a number of significant advantages. The system is simple from the computation and communication point of view. The number of real time operations is limited and the most complex operations are performed off-off line. The inventive e-cash scheme protects the privacy of the user while permitting exposure of the identity of a double spender.

Brief Description of the Drawing

Fig. 1 schematically illustrates a network in which the e-cash scheme of the present invention may be utilized.

Fig. 2 schematically illustrates a payment operation using e-cash in accordance with the present invention.

Fig. 3 schematically illustrates a deposit operation using the e-cash system of the present invention

Fig. 4 schematically illustrates an exchange operation using the e-cash system of the present operation.

Fig. 5 schematically illustrates a withdrawal operation using the e-cash system of the present invention.

Fig. 6 schematically illustrates an operation for generating an initial certificate of a public key of a user in accordance with the invention.

Fig. 7 schematically illustrates an operation for refreshing a certificate of a public key in accordance with the invention.

Fig. 8 and Fig. 9 illustrate a cut-and-choose technique used to prove the P_i is properly structured in the initial certificate and refresh certificate operations of the present invention.

Detailed Description of the Invention

A. The Network Environment

Fig. 1 schematically illustrates a network 10 in which the e-cash of the present invention may be utilized to perform a variety of transactions. The network 10 includes a plurality electronic e-coin processing units such as money modules belonging to users, one or more banks, and a certificate authority.

Illustratively, the network 10 of Fig.1 includes a first portable money module 12 belonging to the user i and a second portable money module 14 belonging to the user j. The money module 12 includes a CPU (e.g., a microprocessor) 16 and a memory 18. The money module 14 includes a CPU 20 and a memory 22. The money module 12 may be temporarily connected via a line 24 to the public switched telephone network 26. The money module 14 may also be temporarily connected via a line 28 to the public switched telephone network 26. Conventional modems (not shown) connect the money modules 12,14 to the lines 24,28. Alternatively, the money modules may be connected to the public switched telephone network via wireless radio channels. Illustratively, the public switched telephone network 26 is an ISDN (Integrated Service Digital Network). The money modules 12 and 14 can communicate with each other via the public switched telephone network 26.

Alternatively, a wireless connection 30 can be established between the money modules 12 and 14. The wireless connection 30 may be established in a cellular network or rely on a direct radio link through the atmosphere between the two money modules. A wireless infrared link may also be established between the two money modules.

It should be noted that the CPU's 16 and 20 of the money module 12 and 14 have limited processing power. In addition, the memories 18 and 22 of the money modules 12 and 14 have limited capacity. Thus, it is desirable for the e-cash transactions of the present invention to require only limited numbers of real time operations at the money modules.

The network 10 also includes a certificate authority station 32. The certificate authority station 32 includes a server 34 and a memory 36. The server 34 is connected to the telephone network 36 by the link 38.

The network 10 also includes a bank station 40. The bank station comprises a server 42 and a memory 44. The server 42 is connected by the link 46 to the telephone network 26.

The network 10 of Fig. 1 is illustrative only. While only two money modules 12 and 14 belonging to users i and j are shown, a network for using e-cash may include a large number of such money modules. In addition, there may be more than one bank.

B. Money Format

As indicated above, each user i has a public key $P_i \equiv \alpha^{si}$ mod p where α and p are universally known and S_i is a secret key. The secret key S_i includes the identity I_i of user i. Illustratively, $S_i = (I_i, R_i)$, where R_i is a random string of bits known only to the user i. In addition, the user i has a certificate cert(i) which certifies that P_i has the identity I_i contained within the exponent S_i. This format is important for the exposure of a double spender of a particular e-coin. Illustratively, the certificate cert(i) is the signature of a certificate authority on $(P_i, 0^\gamma)$, where 0^γ denotes a run of γ zeroes and $30 < \gamma < 50$. For example, cert(i) $\equiv (P_i, 0^\gamma)^{dc}$ mod N_c, where d_c is the secret RSA exponent of the certificate authority and N_c is the modulus of the certificate authority. A detailed process for obtaining the certification is described below in connection with Fig. 6.

A coin of user i has the form (P_i, u, C) where the certified linkage $C=(f(P_i,u,0^\gamma)^{d\$})$ mod$N_\$$, where $u \equiv \alpha^r$ mod p, r is a random element chosen by i separately for each coin and known only to i. The exponent $d_\$$ is a secret RSA exponent of a bank for a particular coin denomination, and $N_\$$ is the bank modulus. The bank also has a public RSA exponent $e_\$$ such that $(m^{d\$})^{e\$}$ mod $N_\$ \equiv$ m, for all m.

C. Payment Transaction

One transaction which can be performed using the e-cash of the present invention is a payment transaction. The payment transaction involves communication between the money module 12 belonging to a payer i and a money module 14 belonging to the payee j. These communications take place via the telephone network 26 or the wireless link 30. The computations required in the payment transaction are performed in the CPU's 18 and 20 of the money modules 12, 14.

The payment operation is illustrated in Fig. 2 and comprises the following steps:

1. The payer i transmits a coin (P_i,u,C) where the certified linkage $C\equiv(f(P_i,u, 0^\gamma)^{d\$}$ $\mathrm{mod}N_\$$ to the payee j.
2. The payee j verifies the coin by verifying the banks RSA signature, i.e., by verifying that $C^{e\$} \equiv (P_i, u, 0^\gamma) \bmod N_\$$. If the verification fails, the payment operation is aborted.
3. If the verification is successful, the payee j picks a random message m.
4. The random message m is transmitted from the payee j to the payer i.
5. The payer i generates an El Gamal signature s=(u,v) on the message m using P_i, S_i, and u. As indicated, P_i and S_i have the form of El Gamal public and secret keys. (Alternatively, an NIST-DSS or Schnorr signature or other scheme from the El Gamal family may be used).
6. The El Gamal signature s is transmitted from the payer to the payee j.
7. The payee j verifies the El Gamal signature s=(u,v). If the signature s is not verified positively, the payment operation is aborted. If the signature is verified positively, the payee j stores the coin (P_i,u,C), signature s, and the message m in the memory 22.

It should be noted that the payee j never learns the identity I_i of the payer i because there is no easy way to correlate the public key P_i with the identity I_i if p is large enough. Thus, privacy of the payer i is maintained.

D. Deposit Transaction

Fig. 3 shows a transaction wherein the payee j deposits the coin (P_i,u,C) received from the payer i in the bank 40. To carry out the deposit operation, the money module 14 of the payee j and the bank 40 communicate via the public switched telephone network 26. The steps in the deposit transaction are as follows:

1. The payee j transmits the coin C and the El Gamal signature s received from the payer i, as well as the message m, to the bank 40.
2. The bank verifies the coin by verifying that $C^{es} \bmod N_s \equiv f(P_i, u, 0^\gamma)$.
3. The bank maintains a list of deposited coins. For each coin, the list includes a message and an El Gamal signature obtained on the message using the El Gamal key and value of u inside the coin. This list is stored in the memory 44. (An expiration date may be added to the coins to limit the size of this list).
4. Using the server 42, the bank 40 compares the coin (P_i,u,C) to the list of already deposited coins stored in the memory 44. If a collision is found, double spending is detected. Then the identity I_i of the payer i is determined. The identity can be determined because two El Gamal signatures on different messages but using the same P_i and u result in exposure of the secret key S_i. Because S_i contains I_i,then I_i is also exposed. This was proven in connection with equations (2) and (3) above. If the coin C is not found in the list, the payer's signature s is verified. Then the coin (P_i,u,C) and associated El Gamal signature s and message m are added to the list maintained at the bank.

5. The payee j has its balance updated by the bank.

It should be noted that the deposit operation does not reveal the identity I_i of the payer i unless the payer is a double spender.

E. Exchange Transaction

Another transaction which can be performed using the e-cash of the present invention is an exchange transaction. The exchange transaction involves a user depositing old e-coins with the bank and withdrawing new e-coins in the same total amount. The purpose of the exchange operation is to perpetuate the privacy of the payer i and payee j. Illustratively, the exchange transaction is performed by communication between the money module 14 of the user j and the bank 40 using the public switched telephone network 26. As shown in Fig. 4, the steps involved in the exchange operation are as follows:

1) The payee j sends to the bank the used coin (P_i, u, C), where the certified linkage $C \equiv (f(P_i, u, 0^\gamma))^{d\$}$ mod $N_\$$, received from payer i and the El Gamal signature s received from payer i along with the message m.

2) The bank verifies the coin by verifying $C^{e\$}$ mod $N_\$ \equiv f(P_i, u, 0^\gamma)$.

3) The bank compares the coin (P_i, u, C) to a list of already deposited coins stored in the memory 44. If a collision is found, double spending is detected. Then the identity of the double spender is determined in the same manner as for the deposit transaction discussed above. If the coin C is not found in the list, the payer's signatures s is verified and the coin C is added to the list maintained by the bank.

4) A certificate, $\text{cert}(j) \equiv (f(P_j, 0^\gamma))^{dc}$ mod N_c and $u' \equiv \alpha^{r'}$ mod p are transmitted from the payee j to the bank.

5) The bank verifies the certificate and forms a new certified linkage C′ to the user j, who then formats a new coin (P_j, u', C')

Note: For this operation the bank never learns the identity of the payer i or the payee j. Nor can the bank associate the coin (P_j, u', C') with any particular user as the coin C′circulates. The reason for this is that the bank has no way to correlate P_i or P_j with I_i or I_j.

The above described three transactions - payment, deposit, exchange - are all performed in real time and require a minimum amount of operations at the money modules.

F. Withdrawal Transaction

Another transaction which can be performed using the e-money of the present invention is withdrawal from the bank. Illustratively, the user i uses the money module 12 to communicate with the bank 40 via the telephone network 26 to perform the withdrawal operation. The steps in the withdrawal operation are shown in Fig. 5 and described below.

1) The user i transmits its identification I_i, an account number and a value to be withdrawn to the bank.

2) The bank verifies the identification I_i and checks the account balance.

3) The user i picks a random x and forms a blinded candidate linkage $W=\chi^{e\$}(P_i,u,0^{\gamma}) \bmod N_{\$}$ and transmits the blinded candidate linkage to the bank.

4) The user i proves to the bank that $P_i \equiv \alpha^{si} \bmod_p$ is properly formatted and that S_i includes I_i. This is done using a zero knowledge proof, or a cut-and-choose technique, for example, so that the bank does not learn P_i. Thus, the bank cannot correlate P_i and the identity of i. Therefore, the privacy of user i is preserved.

5) If the bank rejects the proof, the operation is halted. Otherwise the bank forms $W^{ds} \equiv xf(P_i,u,0^{\gamma})^{ds} \bmod N_{\$}$ and transmits this quantity to the user.

6) The user then forms the coin (P_i,u,C) using the linkage $\equiv W^{ds}/x$

$$\equiv f(P_i,u,0^{\gamma})^{ds} \bmod N_{\$}$$

It should be noted that the withdrawal operation is more complex than the exchange operation because the user i must prove that P_i as incorporated in the blinded candidate linkage is properly formatted without revealing P_i. It is expected that the withdrawal operation may be avoided most of the time. The reason that the withdrawal operation can be avoided is that e-coins can be traded for traceable e-money such as e-checks and then the exchange operation can be utilized.

G. Certification Operation

As indicated above, the e-money system of the present invention makes use of a certification of the key P_i. The certification is carried out off-off line by the certificate authority. The money module of a user i communicates with the certificate authority 32 via the telephone network 26. The steps in the certification process of P_i are illustrated in Fig. 6 and are as follows:

1. The user picks a random x and forms the blinded candidate certificate $Z \equiv x^{ec}f(P_i, 0^{\gamma}) \bmod N_c$.
   The blinded candidate certificate Z is then transmitted to the certificate authority along with an identifying I_i.
2. The user, then proves to the certificate authority that P_i is formatted correctly using for example a zero knowledge proof or cut-and-choose technique so that the certificate authority does not learn P_i and therefore cannot correlate P_i and I_i.

3. If the proof is rejected, the certificate operation is halted. Otherwise, the certificate authority computes Z^{dc} and transmits Z^{dc} to the user i.
4. The user i then computes cert(i) $\equiv Z^{dc}/x \equiv f(P_i, 0^\gamma)^{dc} \bmod N_c$.

Using this certification process, the certificate authority does not learn P_i and, therefore, cannot correlate P_i and I_i. This prevents the certificate authority from learning about the e-cash transactions performed by the user i, thereby protecting the privacy of the user i.

H. Refresh Operation

Because it is possible that the correspondence between P_i and I_i will leak out (e.g. by means external to cryptography), it is desirable to refresh the P_i and cert (i) periodically. The refresh operation is illustrated in Fig. 7 and the steps may be described as follows:

1) The user picks a random x.
2) The user selects a new key $P_i' \equiv \alpha^{s_i'} \bmod p$, $S_i' = (I_i, R_i')$, where R_i' is a fresh string of random bits selected by the user i. Using the key P_i', a new candidate certificate $f(P_i', 0^\gamma)$ is selected. The new candidate certificate is blinded by computing $Y \equiv x^{ec} f(P_i, 0^\gamma)$. Y and the old certificate cert (i) are transmitted to the certificate authority.
3) The user i proves to the certificate authority that P_i and P_i' contain the same I_i, using for an example, a zero knowledge proof or cut and choose technique so that the certificate authority cannot correlate P_i or P_i' with I_i.
4) If the certificate authority rejects the proof the operation is halted. Otherwise the certificate authority computes $(Y)^{dc}$ and transmits this value to the user i.
5) The user i then computes a new certificate

$$cert_2(i) \equiv (Y)^{dc}/x \equiv f(P_i,\ 0^{\gamma})^{dc} \bmod N_{\varsigma}.$$

In short, a unique electronic cash system has been disclosed. The electronic cash system of the present invention protects the privacy of users in legitimate transactions, while at the same time permitting the identity of a double spender of a particular electronic coin to be revealed. These highly beneficial results are achieved through the use of the El Gamal signature scheme and other public key cryptographic techniques.

It should be noted that while certain operations utilized in connection with the invention have been described herein through use of the RSA public key cryptographic technique, other public key cryptographic techniques such as Rabin modular square roots may be used in place of RSA.

Finally, the above described embodiments of the invention are intended to be illustrative only. Numerous alternative embodiments may be devised by those skilled in the art without departing from the spirit and scope of the following claims.

CLAIMS

1. A method for using electronic cash to perform a transaction comprising the steps of

transmitting via a communications link from a first electronic coin processing unit to a second electronic coin processing unit an electronic coin comprising a linkage of a public key of a party and a random element, said linkage being signed using a secret operation of a public key cryptographic system.

2. The method of claim 1 wherein said public key has the form

$$P_i = \alpha^{si} \bmod p$$

where P_i is a public El Gamal Key of a party i, S_i is a secret El Gamal Key of the party i which includes an identity I_i of the party i, and p and α are publicly known numbers, wherein said random element has the form $u \equiv a^r \bmod p$, and where r is a random number chosen by the party i.

3. The method of claim 1 wherein said linkage is signed using an RSA secret exponent of a bank.

4. The method of claim 1 wherein said transmitting step comprises transmitting said electronic coin via a wireless link.

5. The method of claim 1 wherein said transmitting step comprises transmitting said electronic coin via a public switched telephone network.

6. The method of claim 1 wherein said first electronic coin processing unit is a first money module belonging to a first party i.

7. The method of claim 6 wherein said first money module comprises a central processing unit and a memory.

8. The method of claim 6 wherein said second electronic coin processing unit is a second money module belonging to a second party j.

9. The method of claim 8 wherein said transaction comprises transmitting said coin from said first money module of

said first party i to said second money module of said second party j.

10. The method of claims 9 further comprising the steps of

a) transmitting a message m from the party j to the party i,

b) signing the message m at the party i with a signature from the El Gamal family,

c) transmitting the signature to the party j, and

d) verifying the signature at the party j

11. The method of claim 8 wherein said second money module comprises a central processing unit and a memory.

12. The method of claim 1 wherein said first electronic coin processing unit is a money module belonging to a party j and said second electronic coin processing unit is a bank.

13. The method of claim 12 wherein said transmitting step comprises transmitting said electronic coin from said party j to said bank.

14. The method of claim 13 wherein said public key in said electronic coin transmitted from said party j to said bank is the public key of a party i who transferred the coin to the party j.

15. The method of claim 14 further comprising the steps of transmitting from said party j to said bank an El Gamal family signature of the party i on a message m and said message m.

16. The method of claim 15 further comprising the steps of

a) maintaining in a memory at said bank a list of coins and corresponding El Gamal family signatures,

b) comparing said coin transmitted to said bank from said party j with the coins in said list,

c) if there is a collision between said coin, transmitted from said party j and a coin on said list, utilizing the El Gamal family signature transmitted from the party j and the El Gamal family signature of the coin in the list to identify a double spender.

17. The method of claim 16 further comprising the steps of

d) transmitting to said bank from the party j a certificate of a public key of the party j, and

e) transmitting from the bank to the party j a new coin equal in value to the coin originally transmitted from the party j to the bank.

18. A method for detecting the double spending of a particular electronic coin in an electronic coin system where each of the coins comprises a certified linkage of a public key P_i of a user i in which the identity I_i of the user i is embedded.

said method comprising the steps of

a) storing in a memory a list of coins, corresponding messages m, and El Gamal family signatures s on the messages m obtained using the public key and random elements in the coins,

b) using an electronic processor, comparing said particular coin to the coins on the list, and

c) if there is a collision between said particular coin and a coin on said list, using a particular El Gamal family signature of said particular coin on a particular message and the El Gamal family signature and message of said coin on said list to identify a double spender.

19. The method of claim 18 wherein said certified linkage is of the form $C\equiv f(P_i,u,O^{\gamma})d^{\$} \bmod N_{\$}$

where P_i is said public key of said user i.

u is said random element.

O^{γ} is a string of γ zeros.

$d_{\$}$ is the secret RSA exponent of a bank

$N_{\$}$ is a modulus of the bank.

20. The method of claim 18 wherein said public key P_i is of the form

$P_i\equiv\delta^{si} \bmod p$,

where ^{si} is a secret key of the user i and includes the identity I_i of the user i, δ and p are publicly known numbers and said random element is of the form u= δ^r mod p where r is a random chosen number.

21. A method for electronically withdrawing an electronic coin from a bank comprising the steps of

a) using a processor in a money module of a user i, performing a blinding operation to blind a candidate linkage, which blinded candidate linkage includes a public key of the user i of the form $P_i \equiv \alpha^{si}$ mod p, where S_i is a secret key of the user i and contains an identity I_i of the user i, and α and p are publicly known numbers,

b) transmitting via a communication link from the user i to the bank the identity of the user i and the blinded candidate linkage,

c) said money module of said user i providing an indication to said bank that P_i has said form without revealing P_i to said bank,

d) utilizing a processor at said bank, signing said blinded candidate coin using a secret key of said bank and transmitting the signed blinded candidate linkage to said user i, and

e) at said user i, generating a coin from the signed blinded candidate linkage.

22. The method of claim 18 wherein said certified linkage is of the form $C \equiv f(P_i, u, O^{\gamma}) d^{\$}$ mod $N_{\$}$

where P_i is said public key of said user i.

u is said random element.

O^{γ} is a string of γ zeros.

$d_{\$}$ is the secret RSA exponent of a bank

$N_{\$}$ is a modulus of the bank.

23. The method of claim 18 wherein said public key P_i is of the form

$P_i \equiv \delta^{si}$ mod p,
where ^{si} is a secret key of the user i and includes the identity I_i of the user i, δ and p are publicly known numbers and said random element is of the form u= δ^r mod p where r is a random chosen number.

24. A method for certifying a public key of a user of an electronic cash system comprising the steps of

a) utilizing an electronic processor of a user, performing a blinding operation on a candidate certificate to generate a blinded candidate certificate, said blinded candidate certificate including a public key of a user i of the form $P_i \equiv \alpha^{si}$ mod p, where S_i is a secret key of the user i containing an identity I_i of the user i,and α and p are publicly known numbers,

b) transmitting via a communication link, said blinded candidate certificate to a certificate authority,

c) transmitting via said communication link an indication to said certificate authority that P_i contains I_i without revealing P_i to the certificate authority,

d) utilizing a processor at said certificate authority, signing said blinded candidate certificate using a secret key of said certificate authority and transmitting the signed blinded candidate certificate to said user i, and

e) at said user i, generating a certificate from said signed blinded candidate certificate.

25. The method of claim 37 wherein said candidate certificate has the form $f(P_i, O^\gamma)$.

26. A method for refreshing a certificate of a public key of a user in an electronic cash system comprising the steps of:

(a) transmitting from a user i to a certificate authority an old certificate of an old public key P_i of the form $P_i \equiv \alpha^{si}$ mod p, where S_i is an old secret key that includes an identity I_i of the user i, and α and p are public integers,

(b) at the user i, using an electronic processor, selecting a new public key $P_i' \equiv \alpha^{si'}$ mod p where S_i' is new secret key including the identity I_i, and forming a blinded candidate refresh certificate including said new key P_i',

(c) transmitting from said user i to said certificate authority said blinded candidate refresh certificate,

(d) transmitting to said certificate authority an indication that P_i' contains the same I_i as P_i without revealing P_i to said certificate authority,

(e) utilizing an electronic processor at said certificate authority, signing said blinded candidate refresh certificate using a secret key of the certificate authority and transmitting the signed blinded candidate refresh certificate to the user i, and

(f) at said user i, generating a refresh certificate from said signed blinded candidate refresh certificate.

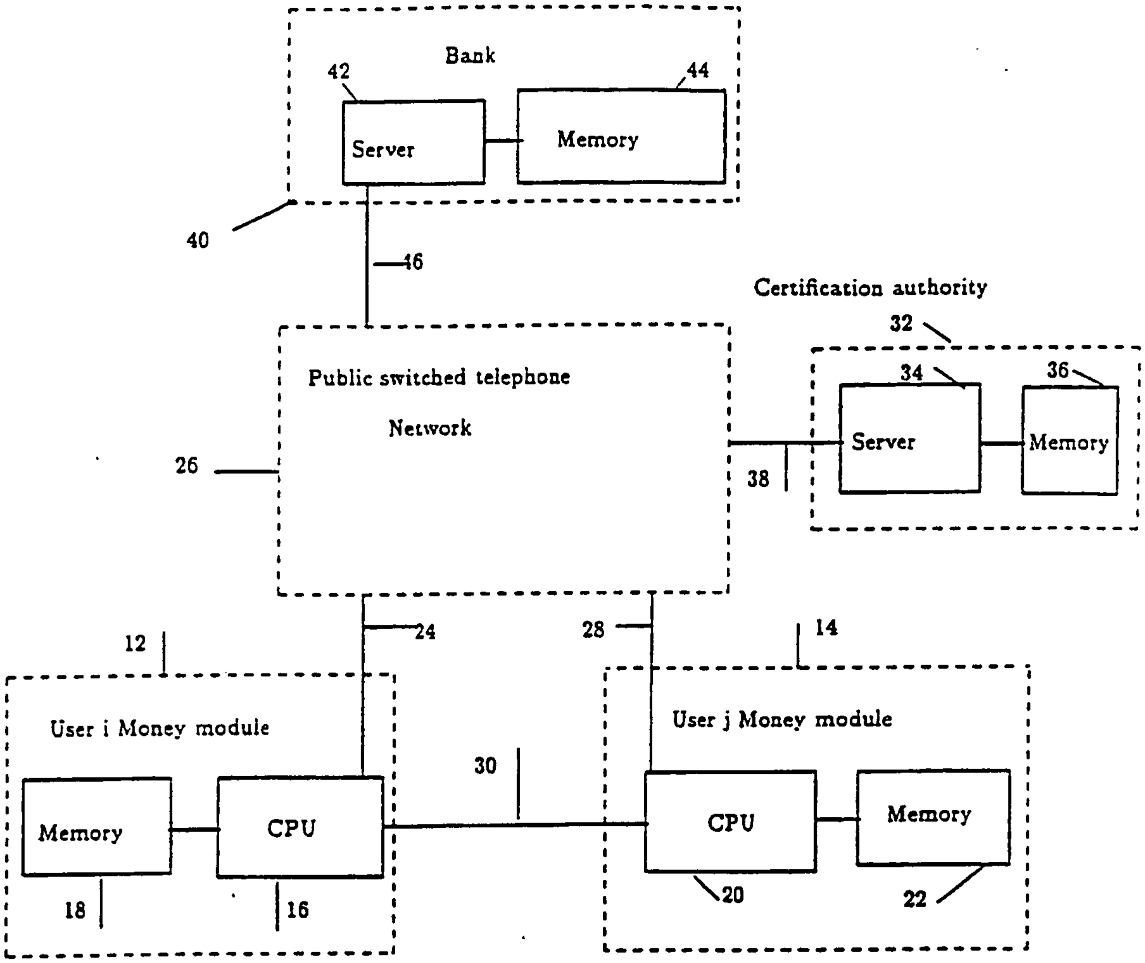

Bank
42
44
Server
Memory
40
46
Certification authority
32
Public switched telephone
Network
34
36
Server
Memory
26
38
12
24
28
14
User i Money module
User j Money module
30
Memory
CPU
CPU
Memory
18
16
20
22

Fig 1

Fig 2

	Payer − i		*Payee − j*
(1)	$C \equiv (f(P_i, u, 0^7))^{d_b} \bmod N_b$	→	
(2)			$C^{e_b} \equiv (f(P_i, u, 0^7)) \bmod N_b$ (abort if not)
(3)			Pick random m
(4)		←	(m)
(5)	S=El-Gamal signature of m using (P_i, S_i, u)		
(6)	(S)	→	
(7)			Verify (S, m, P_i) Abort if negative Else, store (C, S, m)

□

Fig 3

	Payee − j		*Bank*
(1)	Coin C El-Gamal signature S Message m	→	
(2)			Bank verifies coin by verifying $C^{e_b} \equiv (f(P_i, u, 0^7)) \bmod N_b$
(3)			Bank maintains a list of deposited coins, El-Gamal signatures, and messages.
(4)			Coin in list? If yes, abort and compute payer's identity. Else, verify payer's signature. If positive, add coin C to list.
(5)			Update j's balance.

□

Fig 4

	$User - j$		$Bank$
(1)	Coin C El-Gamal signature S Message m	—	
(2)			Verify coin
(3)			Coin in list? If yes, abort and compute payer's identity. Else, verify payer's signature S. If positive, add coin C to list.
(4)	$Cert(i) \equiv (f(P_j, 0^7))^{d_c} \bmod N_c$ $u \equiv a^r \bmod p$	—	
(5)		←	New coin $C' \equiv (f(P_j, u, 0^7))^{d_b} \bmod N_b$
		▯	

Fig 5

	$User - i$		$Bank$
(1)	I_i, account No. value to be withdrawn	—	
(2)			Verify ID, check balance
(3)	Pick random x Form blind candidate coin $w \equiv x^{e_b}(f(P_i, u, 0^7)) \bmod N_b$	—	
(4)	Prove P_i is properly formated.		
(5)		←	If bank rejects proof then halt. Else, compute $w^{d_b} \equiv x(f(P_i, u, 0^7))^{d_b} \bmod N_b$
(6)	$C \equiv w^{d_b}/x \equiv (f(P_i, u, 0^7))^{d_b} \bmod N_b$		
		▯	

Fig 6

	$User - i$		Certification Authority
(1)	Pick a random x Compute $z \equiv x^{e_c}(f(P_i, 0^7)) \bmod N_c$	—	
(2)	Prove P_i is proper		
(3)		←	If proof is rejected halt operation. Else, $(z^{d_c} \bmod N_c)$
(4)	$Cert(i) \equiv z^{d_c}/x \equiv (f(P_i, 0^7))^{d_c} \bmod N_c$		
		▯	

Fig 7

	User − i		Certification Authority
(1)	Pick random x		
(2)	Old $Cert(i) \equiv (f(P_i, 0^7))^{d_e} \bmod N_e$	—	Verif. old Cert.
	Blind new candidate certificate		
	$Y \equiv x^{e_e}(f(P_i', 0^7)) \bmod N_e.$	—	
(3)	Prove to CA that P_i and P_i'		
	have the same I_i in the exponents.		
(4)			If proof is rejected
			halt operation.
			Else, compute
		—	$(Y^{d_e} \bmod N_e)$
(5)	$Cert_2(i) \equiv Y^{d_e}/x \equiv (f(P_i', 0^7))^{d_e} \bmod N_e$		
		□	

Fig 8

	User − i		Certification Authority
Phase I:			
(1)	User-i authenticates herself, (I_i)	—	
(2)	$\{(B_{ij}^{(0)}, B_{ij}^{(1)}) \mid j = 1 \cdots k\}$	—	
(3)		—	$e = (e_1 \cdots e_k)$
(4)	$\{(x_{ij}^{e_j}, R_{ij}^{e_j}) \mid j = 1 \cdots k\}$	—	
(5)			Verify:
			$B_{ij}^{e_j} \equiv_{N_e} (x_{ij}^{(e_j)})^{e_e} \cdot f((\alpha^{S_{ij}})^{(e_j)}, L), \quad j = 1 \cdots k$
(6)			$B_i \equiv_{N_e} \prod_{j=1}^{k} B_{ij}^{(e_j)}$ (*)
(7)		—	$C_i \equiv_{N_e} B_i^{d_e}$
(8)	$D_i \equiv_{N_e} C_i \cdot (\prod_{j=1}^{k} x_{ij})^{-1}$		
Phase II:			
(9)	Make anonymous call to CA.		
(10)	$D_i, \quad \{P_{ij}^{(e_j)} \mid j = 1 \cdots k\}$	—	
(11)			Verify (partial) structure and signature.
(12)	For $j = 1 \cdots k$		
	prove that in $S_{ij}^{(e_j)}$		
	all the I-fields except the j'th		
	are zeroes.		Verify
(13)		—	$E_i \equiv_{N_e} (f((\prod_{j=1}^{k} P_{ij}^{(e_j)} \bmod p), L)^{d_e}$
		□	

Fig 9

	$User - i$		Certification Authority
(1)	Make anonymous call to CA (old E'_i, $\{P'_{ij} \| j = 1 \cdots k\}$)	—	
(2)			Verify (partial) structure and signature.
(3)	$\{B^q_{ij} \| q = 0, 1: \ j = 1 \cdots k\}$	—	
(4)		←	$e \in_R \{0, 1\}^k$ $e = (e_1 \cdots e_k)$
(5)	$\{(P^{(e_j)}_{ij}, x^{(e_j)}_{ij}) \| j = 1 \cdots k\}$	—	
(6)			Verify (partial) consistency with $B^{(e_j)}_{ij}, j = 1 \cdots k$
(7)		Both compute $P'_i \equiv_p \prod_{j=1}^k P'_{ij}; \ P^{(e)}_i \equiv_p \prod_{j=1}^k P^{(e_j)}_{ij}; \ A \equiv_p P'_i / P^{(e)}_i$	
(8)	Prove that $A \equiv_p \alpha^\delta$, where δ is short.		
(9)		Proceed as in Init. cert. from (*). ▯	

INTERNATIONAL SEARCH REPORT

International application No.
PCT/US95/02007

A. CLASSIFICATION OF SUBJECT MATTER

IPC(6) :HO4K 1/00
US CL :380/30
According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

U.S. : 380/22, 23, 24, 25, 28, 30

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	US, A, CHAUM; "Untraceable Electronic Cash Proceedings of CRUPTO 1988 pp 1-8	1-26
Y	US, A, ELGAMUL; "A Public Key Cryptosystem and a Signature Scheme Based on Discrete Logorithms IEEE Transaction Information Theory; 1985 vol. IT31 pp 469-472.	1-26

□ Further documents are listed in the continuation of Box C. □ See patent family annex.

*	Special categories of cited documents:	"T"	later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
"A"	document defining the general state of the art which is not considered to be part of particular relevance		
"E"	earlier document published on or after the international filing date	"X"	document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
"L"	document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)	"Y"	document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art
"O"	document referring to an oral disclosure, use, exhibition or other means		
"P"	document published prior to the international filing date but later than the priority date claimed	"&"	document member of the same patent family

Date of the actual completion of the international search

27 MARCH 1995

Date of mailing of the international search report

24 APR 1995

Name and mailing address of the ISA/US
Commissioner of Patents and Trademarks
Box PCT
Washington, D.C. 20231

Facsimile No. (703) 305-3230

Authorized officer

TOD R. SWANN

Telephone No. (703) 308-0475